

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)

115274-008

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

on _____

Signature _____

Typed or printed
name _____

Application Number

09/054,180

Filed

April 1, 1998

First Named Inventor

Brian J. Reistad et al.

Art Unit

3621

Examiner

Firmin Backer

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).

Note: No more than five (5) pages may be provided.

I am the _____

☐ applicant/inventor.☐ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed.
(Form PTO/SB/96)☒ attorney or agent of record. 48,196
Registration number _____☐ attorney or agent acting under 37 CFR 1.34.

Registration number if acting under 37 CFR 1.34 _____



Signature

Peter Zura

Typed or printed name

312-807-4208

Telephone number

September 14, 2006

Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required.
Submit multiple forms if more than one signature is required, see below*.

☒ *Total of 1 forms are submitted.

This collection of information is required by 35 U.S.C. 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Brian J. Reistad et al.
Appl. No.: 09/054,180
Conf. No.: 2217
Filed: April 1, 1998
Title: ELECTRONIC COMMERCE SYSTEM
Art Unit: 3621
Examiner: Firmin Backer
Docket No.: 0115274-0008

MAIL STOP AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PRE-APPEAL BRIEF REQUEST FOR REVIEW

EXPEDITED PROCEDURE REQUESTED, TECHNOLOGY CENTER 3600

Sir:

This request is submitted in response to the Final Office Action dated June 14, 2006. This request is filed contemporaneously with USPTO form PTO/SB/33, "Pre-Appeal Brief Request for Review" and form PTO/SB/31, "Notice of Appeal."

Remarks begin on page 2 of this paper.

REMARKS

Claims 1-3 and 9 remain in the present application. Independent claims 12-14, 34-36, 39-41 and claim 61-63 are the focus of this request. Applicant respectfully notes that this is the second Appeal of this application based on prior art, which in the Applicant's opinion detailed below, bears little relation to the claimed features.

Claims 12-36 and 39-63 were rejected under 35 U.S.C. §102(e) as being clearly anticipated by *Barnett et al.* (US Patent 6,321,208). Applicant submits these rejections are improper and respectfully requests reversal by this Board.

Specifically, *Barnett* does not disclose a client computer configured for, or the step of, transmitting an order acceptance request over a packet-switched network that includes a plurality of modular elements, with each modular element individually protected by an imbedded cryptographic security code, as recited in claims 12-14, 34-36, 39-41 and 61-63. Also among the features of the pending claims is a server configured to, or the step of, transmitting an order acceptance response to a client, the order acceptance response also including a plurality of modular elements whose individual integrity is protected by embedding a cryptographic security code within each modular element.

The teaching of *Barnett* was detailed in the Applicant's Response dated March 29, 2006. Generally, *Barnett* teaches a central server that (1) collects information and identification from users accessing the server requesting coupons, (2) encodes user and product information into a barcode, (3) formats the barcode and other text/graphics into the form of a printable coupon, and (4) transmits the printable coupon over the network to the user for subsequent printing and redemption (col. 4, lines 40-60; col. 5, lines 22-33; col. 7, lines 6-17, 21-25).

In the Office Action, and during the Examiner Interview conducted August 31, 2006, it was stated by the Examiner that the process of "encoding" data into a printable barcode format to create a "virtually fraud-proof" coupon was the equivalent of cryptographic encoding. This is simply incorrect and misstates the teaching of the underlying technology. Bar-coding is premised upon *symbolology*, which deals with encoding digits/characters of a message, as well as the start and stop markers, into bars and space. The symbolology of the barcode (e.g., UPC, code 128, etc.) is merely a

machine-readable representation of information in a visual format on the physical surface of a coupon (such as ref. 90 of *Barnett*). There is no encryption or ciphering of the data whatsoever; it is merely converted into a format that can be read quickly and easily by a fixed-light or laser scanner, instead of being manually read by a merchant. Furthermore, the Office Action fails to identify what teaching in *Barnett* discloses a plurality of modular elements whose individual integrity is protected by embedding a cryptographic security code within each modular element. Under the barcode conversion of *Barnett*, *all of the coupon information is jointly translated into a singular barcode* (col. 7, lines 22-35).

Furthermore, the references in *Barnett* to the coupon being “virtually fraud-proof” has nothing to do with the integrity of the data being transmitted over the network. Instead, *Barnett* provides and stores unique identity information to each coupon (e.g., user information, expiration date), where the coupon redemption center may control the time (i.e., before an expiration date) or manner (i.e., only one coupon redemption per user) in which the coupon is redeemed based on this identity information (see col. 11, lines 2-23). The “fraud” referred in *Barnett* deals with instances where (1) photocopies are made of coupons in an effort to obtain multiple redemptions (col. 11, lines 11-23), or (2) someone other than the user (who presumably can’t provide identification to the merchant at the time of redemption) is attempting to redeem a prohibited coupon (col. 7, lines 21-34).

In contrast, the present invention recites *cryptography* in the form of security codes embedded within each of the plurality of modular elements, at least one of the modular elements individually protected by a cryptographic security code being a digital coupon. As is known in the art, cryptography deals with the secure encoding and authentication of the data itself. Applicant notes that each of the above claims recite the “authentication of the cryptographic security codes embedded within each of the modular elements.” The present specification describes, as an example, the use of key authentication, such as SSL, which contain cryptographic protocols which provide secure communications on the Internet (page 9, lines 6-29; see also page 19, lines 21-28). Under the example of SSL, only the server is authenticated (i.e. its identity is ensured) while the client remains unauthenticated. For mutual authentication, clients must be provided with public key infrastructure (PKI) deployment. The protocols allow client/server applications to communicate in

a way designed to prevent eavesdropping, tampering, and message forgery during the transmission and receipt of a commercial transaction that occurs over the Internet. Claims 35 and 62 specifically recite the use of digital signatures, and claims 36 and 63 specifically recite the use of message authentication codes.

This is neither taught nor suggested in *Barnett* – as discussed above, *Barnett's* system does not conduct commercial transactions over the Internet using the coupons; the entire disclosure is premised entirely on the user printing and physically redeeming the coupon at a retail store or coupon redemption center through the use of barcode scanning. *Barnett* briefly mentions that coupons may be redeemed “electronically” (see FIG. 9, col. 11, lines 29-42), however, it is clear from the disclosure that the “electronic” redeeming of coupons involves the transmission and storage of the coupon at the retail center, where the retail center prints and scans the coupon on location (“[t]hus, the printable coupon data generation routine **32d** combines all this information and generates a record indicative of the unique coupon to be printed”). Even if *Barnett* used technology such as PKI certificates, the entire purpose of such coding would be lost upon subsequent barcoding and printing of the user information.

As *Barnett* does not conduct transactions of the products underlying the printed coupons, *Barnett* also fails to teach or suggest the processing and negotiation of electronically authenticated coupons. The present claims recite that the order acceptance request is authenticated and processed to contain a discreet message transmitted during a negotiation phase of a transaction that includes a plurality of modular elements whose individual integrity is protected by embedding cryptographic security codes within each of the modular elements. *Barnett* is completely silent as to how each of the user information is individually protected through the use of barcodes.

Also, claims 12 and 39 recite that the client computer is programmed to receive the digital coupon, protected by a cryptographic security code, “from another computer.” During the Examiner interview, it was posited by the examiner that the term “another computer” was broad, and that, using a commensurately and “reasonably” broad interpretation, “another computer” was being interpreted as the “server computer.” Applicant respectfully submits that this interpretation is simply wrong and contradicts every convention of claim interpretation. “Another computer” should mean simply that - a computer that is neither the client computer nor the server computer. An

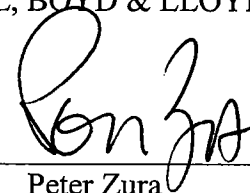
exemplary disclosure of this interpretation may be found in the specification on page 9, lines 29-32. *Barnett* clearly does not disclose this feature, as the entire teaching is premised on providing barcoded coupons from the same central server (see Abstract, col. 4, lines 40-52).

Furthermore, claims 13 and 40 further recite that the authenticated coupons are accepted “without regard to the identity of the coupon holder.” These elements are clearly not taught or suggested in the disclosure of *Barnett*. As was explained during the Interview, Barnett states that the identification of the user is required to make each coupon “unique” and to provide added security for each issued coupon (col. 7, lines 21-31). Thus, Barnett clearly teaches away from the claimed features.

In light of the above, Applicants respectfully submit that independent claims 12-14, 34-36, 39-41 and claim 61-63 of the present application as well as all claims that depend directly or indirectly therefrom are both novel and non-obvious over the art of record. Accordingly, Applicant respectfully requests the rejection be reversed and that a timely Notice of Allowance be issued in this case. If any fees are due in connection with this application as a whole, the office is hereby authorized to deduct said fees from Deposit Account No.: 02-1818.

Respectfully submitted,
BELL, BOYD & LLOYD LLC

BY



Peter Zura

Reg. No. 48,196

Customer No.: 29177

Phone: (312) 807-4208

Dated: September 14, 2006